HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 200309309-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Amit RAIKAR et al.

Confirmation No.: 7736

Application No.: 10/600,113

Examiner: David G. Cervetti

Filing Date: June 20, 2003

Group Art Unit: 2136

Title: AN INTEGRATED INTRUSION DETECTION SYSTEM AND METHOD

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on 09/04/2007.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month $120	☐ 2nd Month $450	☐ 3rd Month $1020	☐ 4th Month $1590

☐ The extension fee has already been filed in this application.

☑ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $500. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

☑ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450

Date of Deposit: 11/05/2007

OR

☐ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.

Date of facsimile:

Typed Name: Ilene L. Fish

Signature: Ilene L. Fish

Respectfully submitted,
Amit RAIKAR et al.

By _____

John P. Wagner, Jr.

Attorney/Agent for Applicant(s)

Reg No. : 35,398

Date : 11/05/2007

Telephone : 408-377-0500

Table of Contents

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellant:	Raikar et al	Patent Application	
Serial No.:	10/600,113	Group Art Unit:	2136
Filed:	June 20, 2003	Examiner:	Cervetti, David Garcia

For: AN INTEGRATED INTRUSION DETECTION SYSTEM AND METHOD

Appeal Brief

Real Party in Interest

The assignee of the present invention is Hewlett-Packard Company.

Related Appeals and Interferences

There are no related appeals or interferences known to the Appellant.

Status of Claims

Claims 1-20 remain pending. Claims 1-20 have been rejected. This appeal involves Claims 1-16.

Status of Amendments

All proposed amendments have been entered. An amendment subsequent to the Final Action has not been filed. However, a terminal disclaimer has been filed herewith to overcome a double patenting rejection.

Summary of Claimed Subject Matter

Independent Claims 1 and 8 of the present application pertain to various embodiments for intrusion detection.

At least one embodiment of Claim 1 "An integrated intrusion detection method" is depicted in Figure 2. In one embodiment (as shown in at least Figure 2, method 200 and page 15, lines 20-24), the method 200 includes gathering information from a plurality of different types of intrusion detection sensors (Figure 2, element 210 and page 16, lines 1-18); processing the information, wherein the processing provides a consolidated correlation of the information (Figure 2, element 220 and page 16, line 20- page 18, line 12); assigning a response corresponding to said information (Figure 2, element 230 and page 20, line 14- page 21, line 2); and implementing the response (Figure 2, element 240 and page 21, line 4- page 22, line 6).

At least one embodiment of Claim 8 "a computer usable storage medium having computer readable program code for causing a computer system to implement intrusion detection" is depicted in Figure 1A (described in page 7, line 15 –page 11, line 10). The computer usable storage medium having computer readable program code embodied therein for causing a computer system to implement intrusion detection instructions includes a data collection module 103 (page 9, line 12) for receiving information from a plurality of different types of intrusion detection sensors, wherein the information indicates potential security issues; an integration module 104 (page 9, line 12) for integrating the information in a network application management platform; a reaction determination module 105 (page 9, line 12) for determining appropriate response to indication of the

potential security issues; and a reaction direction module 107 (page 9, line 12) for directing the response.

Grounds of Rejection to be Reviewed on Appeal

1. In paragraph 16 of the Final Office Action, Claims 1-20 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. patent application publication no. 2003/0188189 by Desai (referred to hereinafter as "Desai").

Arguments

1. Whether Claims 1-20 are anticipated by Desai under 35 U.S.C. 102(e).

A. Claim Features are not Met by the Cited References

Appellants respectfully submit that the rejection of Claims 1-20 is improper as the rejection of Claims 1-20 does not satisfy the requirements of a *prima facie* case of anticipation under 35 U.S.C. § 102(b) as claim features are not met by the cited reference.

According to the Federal Circuit, "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." /Verdegaal Bros. v. Union Oil Co. of California/, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). ... "The identical invention must be shown in as complete detail as is contained in the ... claim." /Richardson v. Suzuki Motor Co/., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

Appellants respectfully submit that Desai does not teach or suggest, among other things, "gathering information from a plurality of different types of intrusion detection sensors," (emphasis added) as recited by Claim 1.

The Office Action asserts that Desai teaches "gathering information from a plurality of different types of intrusion detection sensors," (emphasis added) as recited by Claim 1 at paragraphs 0044-0049. Paragraphs 0044-0049 refer to multi-vendor/multi-platform devices. Paragraph 0083 of Desai provides examples of these devices as "firewalls, routers, hosts, IDS..." However, Desai's "devices" are not examples of "a plurality of different types of intrusion detection sensors."

The Examiner submits that Desai's Figure 1 shows a plurality of different types of sensors (e.g., that events collected at host IDS 17, network IDS, server, are received at collector 20). Appellants respectfully disagree.

As stated, Desai's "devices" are not examples of "a plurality of different types of intrusion detection sensors," (emphasis added) as claimed. Element 20 of Desai is merely a log collector and is not a sensor of any type.

Desai states in paragraph [0047] "a second advantage is that no additional hardware sensors need to be purchased and placed at the end user's premises." Appellants submit that Desai actually teaches away from the feature "gathering information from a plurality of different types of intrusion detection sensors," (emphasis added) as recited by Claim 1.

Consequently, Claim 1 should be patentable over Desai for at least the reason that Claim 1. Independent Claim 8 should be patentable for similar reasons that Claim 1 should be patentable.

Claims 2-7 depend on Claim 1. Claims 9-16 depend on Claim 8. These dependent claims include all of the limitations of their respective independent claims. Further, these dependent claims include additional limitations which further make them patentable. Therefore, these dependent claims should be patentable for at least the reasons that their respective independent claims should be patentable.

In summary, the Appellants respectfully request that the Board reverse the Examiner's rejections of Claims 1-16.

The Appellants wish to encourage the Examiner or a member of the Board of Patent Appeals to telephone the Appellants' undersigned representative if it is felt that a telephone conference could expedite prosecution.

Respectfully submitted,

WAGNER BLECHER LLP

Date: 11/05/2007

John P. Wagner, Jr.
Registration Number: 35,398

WAGNER BLECHER LLP
Westridge Business Park
123 Westridge Drive
Watsonville, CA 95076
408-377-0500

Claims Appendix

1. An integrated intrusion detection method comprising:

gathering information from a plurality of different types of intrusion detection sensors;

processing said information, wherein said processing provides a consolidated correlation of said information;

assigning a response corresponding to said information; and

implementing said response.

2. An integrated intrusion detection method of Claim 1 wherein said information includes intrusion detection alerts.

3. An integrated intrusion detection method of Claim 2 further comprising centrally tracking information associated with intrusion detection alerts from said plurality of different types of intrusion detection sensors.

4. An integrated intrusion detection method of Claim 3 wherein said tracking information associated with intrusion detection includes assigning severity assignments standardized across said plurality of different types of intrusion detection sensors.

5. An integrated intrusion detection method of Claim 2 wherein said intrusion detection alerts are correlated based upon various alert attributes.

6. An integrated intrusion detection method of Claim 2 wherein said response conforms to an enterprise wide strategy.

7. An integrated intrusion detection method of Claim 1 further comprising managing said intrusion detection sensors.

8. A computer usable storage medium having computer readable program code embodied therein for causing a computer system to implement intrusion detection instructions comprising:

a data collection module for receiving information from a plurality of different types of intrusion detection sensors, wherein said information indicates potential security issues;

an integration module for integrating said information in a network application management platform;

a reaction determination module for determining appropriate response to indication of said potential security issues; and

a reaction direction module for directing said response.

9. A computer usable storage medium of Claim 8 wherein said information includes intrusion detection system alert data.

10. A computer usable storage medium of Claim 8 wherein said integration module selects a hook in an intrusion detection system.

11. A computer usable storage medium of Claim 8 wherein said data collection module logs alerts from said plurality of different types of intrusion detection sensors.

12. A computer usable storage medium of Claim 8 wherein said alerts are provided by a simple network management protocol (SNMP), a system log and an application program interface.

13. A computer usable storage medium of Claim 8 wherein said integration module includes analyzing a plurality of manners in which an alert can be provided and selecting the manner that is the most secure with the least dependencies in a communication path.

14. A computer usable storage medium of Claim 8 wherein said integration module utilizes a network application management platform to log information.

15. A computer usable storage medium of Claim 14 wherein:

an open view operation simple network management protocol trap is utilized to handle simple network management protocol trap based alerts;

an open view operation log file encapsulator handles system log based alerts; and

an open view message interceptor handles application program interface propagated alerts with the help of an operation message mechanism.

16. A computer usable medium of Claim 14 wherein a secure open view template configuration is utilized to log information and the one message group is configured for handling intrusion detection system alerts and another message group is configured for handling intrusion detection system errors.

Evidence Appendix

None

Related Proceedings Appendix

None